# 6. Nmap Live Host Discovery

## 🔍 Nmap & Network Scanning

---

### 1. **What is Nmap?**

- **Nmap (Network Mapper)** is an open-source network scanning and security auditing tool.
- Designed for **network discovery** and **security auditing** by identifying live hosts, open ports, running services, and OS information on target machines.
- Widely used for **penetration testing**, network inventory, managing service upgrade schedules, and monitoring host or service uptime.

---

### 2. **How to Use Nmap?**

- Basic syntax:

  ```
  nmap [options] <target>
  ```

- Examples:
  - Scan a single IP:
    `nmap 192.168.1.10`
  - Scan a range of IPs:
    `nmap 192.168.1.1-254`
  - Scan entire subnet:
    `nmap 192.168.1.0/24`
  - Scan specific ports:
    `nmap -p 80,443 192.168.1.10`
  - Aggressive scan (includes OS detection, version detection, script scanning):
    `nmap -A 192.168.1.10`

---

### 3. **How Does Nmap Scan Work?**

- Nmap sends packets to target(s) and analyzes responses to determine:
  - Which hosts are up (live)
  - Which ports are open, closed, or filtered
  - What services and versions are running
  - Operating system details (fingerprinting)
- Different scan techniques probe the network at various layers using TCP, UDP, and ICMP.

---

### 4. **What are Subnetworks?**

- Also called **subnets**, subnetworks divide a larger network into smaller, manageable sections.
- A subnet is identified by a **network address** and a **subnet mask** (e.g., `192.168.1.0/24`).
- Purpose: improve network performance, security, and management by isolating broadcast domains.

## 5. **How to Enumerate Targets?**

- Target enumeration is the process of identifying all hosts within a network range or domain to scope the attack surface.
- Methods include:
  - Ping sweeps (ICMP echo requests)
  - ARP scans (for local networks)
  - DNS queries and subdomain enumeration
  - Port scanning to identify live hosts

## 6. **What is ARP Scan?**

- **Address Resolution Protocol (ARP) Scan** is used to identify devices on the same local subnet.
- Sends ARP requests to IP addresses in a range and listens for ARP replies to determine live hosts.
- Very reliable and fast for local network host discovery because ARP is fundamental to LAN communication.

## 7. **What is ICMP Echo Scan?**

- Sends ICMP Echo Request packets ("ping") to target IPs.
- Targets replying with Echo Reply are considered alive.
- Simple and widely supported but often blocked by firewalls or disabled on hosts for security.

## 8. **What is ICMP Timestamp Scan?**

- Sends ICMP Timestamp Request packets to targets.
- Intended to retrieve the system clock time from the target.
- Less common in modern scanning because many systems disable timestamp responses for security.

## 9. **What is ICMP Address Mask Scan?**

- Sends ICMP Address Mask Request to get subnet mask information from the target.
- Rarely used now, and many systems do not respond for security reasons.

## 10. **What is TCP SYN Ping Scan?**

- Sends TCP SYN packets to a specified port (usually port 80 or 443).
- If SYN-ACK received, host is up; if RST received, port is closed but host is up.

- Faster than full TCP connect scan because it does not complete the TCP handshake (also called "half-open" scan).

---

## 11. What is TCP ACK Ping Scan?

- Sends TCP ACK packets to target port(s).
- Helps determine firewall rules and whether ports are filtered (no response), unfiltered (RST response).
- Used mainly for firewall rule discovery rather than host discovery.

---

## 12. What is UDP Ping Scan?

- Sends UDP packets to the target, typically empty or with specific payloads.
- If ICMP port unreachable is received, the port is closed; no response may indicate open or filtered ports.
- Slower and less reliable because UDP is connectionless and many firewalls block UDP.

---

## 13. What Can Nmap Detect?

- **Live hosts** on a network
- **Open, closed, filtered ports**
- **Service versions** running on open ports
- **Operating system and hardware details** (OS fingerprinting)
- **Firewall rules and filtering** behavior
- **Vulnerabilities and scripts** using NSE (Nmap Scripting Engine)
- **Network topology** and route tracing

---

## 14. How to Scan an IP Address with Nmap

```
nmap 192.168.1.10
```

- Performs a default scan to check for open TCP ports and live host detection.

---

## 15. How to Check Ports with Nmap

- To scan specific ports or a range:

  ```
  nmap -p 22,80,443 192.168.1.10
  nmap -p 1-1000 192.168.1.10
  ```

- To scan all ports:

  ```
  nmap -p- 192.168.1.10
  ```

- Use service/version detection for detailed info:

```
nmap -sV 192.168.1.10
```

---